# Set of equipment for secure direct information transfer over the Internet

The subject of the invention is a set of equipment for secure direct information transfer over the Internet, which contains information transmitting terminal devices suitable for collaborating with an information forwarding network, taking part in the information traffic, the individual information transmitting terminal devices are equipped with a sender partial unit, a receiver partial unit and a storage partial unit comprising an ID-register containing a device identification signal, a C-register suitable for storing a coding key and a D-register suitable for storing a decoding key, where the C-register containing the coding key is in connection with the sender partial unit, and a coding key and a collaborating decoding key are allocated to the individual information transmitting terminal devices.

Due to technical development, especially the development of computer technology and telecommunication electronic equipment are becoming widely used, with the help of which sound and other signal transmission solutions can be realised. In some of these solutions not the ordinary public telecommunication networks are used, and in certain cases, e.g.: for transmitting bank information and making transactions, the transmitted data is coded or encrypted.

International patent No. WO 00/41383 describes a solution with the help of which, in the case that there is appropriate private branch exchange between two telephone sets, the communication chain can be established in a way that after initiating a call first the control unit of the branch exchange finds a remote access database indexing telephone numbers and Internet addresses, there it tries to find the called number, and if it can identify it, then reading the Internet address belonging to the telephone number it established the telephone call over the Internet rather than over the public telephone network, and if it does not find such a telephone number – Internet identifying connection, then it establishes the telephone call over the ordinary public telephone network.

However, the disadvantage of the solution is that if there is no Internet access to the dialled telephone number, then the connection is established in the ordinary way, over the public telephone network, which always results in extra costs for the calling party.

A further disadvantage is that for a cost friendly solution, beside the Internet accessibility of the calling and the called party, traditional telephone connection is also needed, and even individual special private branch exchanges need to be established, which results in a significant increase of the investment costs and also requires further operation and maintenance expenses.

Another significant disadvantage of the solution is that the encryption of the data traffic connection is not solved, and so the traffic can be tapped, it is easily accessible for unauthorised third parties, and by this the established signal forwarding line cannot be used for transmitting optional data.

Another solution is described in international patent application No. WO99/62222 relates to the encryption of telephone traffic. Its main point is that the individual users are given their own password, which they must enter for the central unit in every case after they log in, for the purpose of identifying themselves. The identified users are provided with limited access time from the central unit, during which time their data traffic is encrypted.

However, the greatest disadvantage of this solution is that the period of encrypted data traffic is restricted in time, which in the case when longer connection is needed excludes the possibility of confidential information transfer.

A further disadvantage is that in this case the users must log in the system themselves, and then they must send the central unit a password, which was given to them, so other parties may also know it, and because of the possibility of using a password accessible to other parties confidential data traffic becomes uncertain, and it becomes questionable whether this channel can be used exclusively by a given device or user.

On the basis of the above our aim with the invention was to overcome the deficiencies of the known solutions and to create a set of equipment with the help of which a connection

realising sound, signal or other data traffic can be established in a way identical to ordinary telephoning, so that encrypted information traffic becomes possible independently from the time needed for the connection, during its complete period, and such use always takes place over the Internet, avoiding the public telephone network, which always involves using costs.

The idea behind the invention is based on the recognition that if a suitably constructed central computer unit and terminal devices suitable for establishing Internet-based connection are provided with coding and decoding keys in a way different from the known solutions, then a situation can be achieved where Internet-based communication can be realised in the course of which the sound, still picture, moving picture, signal or other data traffic between the calling party and the called party in connection with each other takes place in an encrypted way impossible to disassemble from the time when the connection is established until it is ended, so that the users of the system do not have any encryption keys or passwords that could be appropriated and by this could endanger the integrity of the network, furthermore the central computer unit in itself is suitable for controlling and managing communication between the terminal devices, and so the task can be solved.

In accordance with the set aim the set of equipment according to the invention for secure direct information transfer over the Internet, – which contains information transmitting terminal devices suitable for collaborating with an information forwarding network, taking part in the information traffic, the individual information transmitting terminal devices are equipped with a sender partial unit, a receiver partial unit and a storage partial unit comprising an ID-register containing a device identification signal, a C-register suitable for storing a coding key and a D-register suitable for storing a decoding key, where the C-register containing the coding key is in connection with the sender partial unit, and a coding key and a collaborating decoding key are allocated to the individual information transmitting terminal devices, – is constructed in a way that the storage partial unit of each information transmitting terminal device is completed with one or more temporary storage registers for the temporary storage of the coding keys of other information transmitting terminal devices, while the information forwarding network is completed with at least one central traffic co-ordinating unit, the central traffic co-ordinating unit has an MD-register storing a master decoding key and a memory unit containing base cells for storing the coding keys belonging

to the individual information transmitting terminal devices, and a master coding key collaborating with the master decoding key is allocated to the central traffic co-ordinating unit, and the C-registers of the information transmitting terminal devices are provided with a master coding key collaborating with the master decoding key stored in the MD-register of the central traffic co-ordinating unit.

A further criterion of the set of equipment according to the invention may be that the temporary storage registers of the information transmitting terminal devices are connected to the sender partial unit.

In the case of a possible construction of the set of equipment the central traffic co-ordinating unit is provided with an MC-register storing a master coding key.

In another different realisation of the invention in the storage partial unit of the individual information transmitting terminal devices there is only information free from the given information transmitting terminal device's own coding key.

The greatest advantage of the set of equipment according to the invention is that with its use connection between the calling party and the called party can be established with simple means, as in the case of ordinary telephone use, but the costs of information flow are significantly lower, while it is guaranteed that the flow of data remains encrypted during the complete period of the connection.

It must also be regarded as an advantage that due to the information transmitting terminal device belonging to the set of equipment no further expensive additional elements need to be acquired, operated or maintained, which has a favourable influence on the expenses in connection with the use of the equipment.

It must also be regarded as an advantage that the specially constructed information transmitting terminal device itself, together with the central traffic co-ordinating unit, realises the encrypting of the data traffic, and so there is no need for a code, identifier or other additional key given to the users, also accessible to unauthorised parties. Another

advantage deriving from this is that it cannot happen that the users cannot enter the system, because they forgot their own code.

A further favourable characteristic of the invention is that the data traffic between the two end points does not take place through a central exchange, which accelerates the flow of information and improves the security of the system, makes the data impossible to disassemble and makes the system impossible to tap.

It is also a disadvantage that as a result of the special nature of the set of equipment according to the invention the terminal devices are impossible to use, if the central computer unit is avoided, which results in that the users of the terminal devices can enter the system only with the approval of the operator of the central computer unit.

A further advantage is that the set of equipment can be installed independently from the manufacturer so that the terminal devices and the central computer unit is uploaded with key pairs by a given operator, and so a closed network can be created, which makes communication possible only for a certain group of users.

Below the set of equipment according to the invention is described in detail in connection of a construction example, on the basis of a drawing. In the drawing

Figure 1 shows a schematic picture of the arrangement of the set of equipment according to the invention.

Figure 1 shows a version of the set of equipment according to the invention, in the case of which – for the sake of simplicity – only one call initiating information transmitting terminal device 10 and one call receiving information transmitting terminal device 20 is detailed. However, it is clear that the set of equipment can contain an optional number of information transmitting terminal devices 10. The number of information transmitting terminal devices is only restricted by the capacity of the central traffic co-ordinating unit 40.

Connection between the information transmitting terminal device 10 and the information transmitting terminal device 20 is established by the information forwarding network 30, with the help of the central traffic co-ordinating unit 40. The information forwarding

network 30 can be an optional communication network, which in this case can mean a wired or wireless, private or public network. The only requirement with respect to the information forwarding network 30 is that it should be suitable for transmitting the signals to be forwarded at a high data rate used in telecommunication, possibly free from distortion.

It can be seen in figure 1 that the central traffic co-ordinating unit 40 is a high-capacity computer device, which has an MC-register 41 and an MD-register 42 on the one part and contains a memory unit 43 on the other part. In the MC-register 41 there is a master coding key 41a, while in the MD-register 42 there is a master decoding key 42a. This unique key-pair enables the information transmitting terminal device 10 and the information transmitting terminal device 20 to realise encrypted data traffic with the central traffic co-ordinating unit 40. In the memory unit 43 of the central traffic co-ordinating unit 40 there is a base cell 43a and another base cell 43b, in which the coding key 16 of the information transmitting terminal device 10 and the coding key 26 of the information transmitting terminal device 20 can be found in a resident way.

However, it must be pointed out here that the master coding key 41a and the MC-register 41 containing it 41 does not necessarily have to be situated in the central traffic co-ordinating unit 40. The MC-register and the master coding key 41a can be situated remote from the central traffic co-ordinating unit so that the master coding key 41a and the master decoding key 42a are not accessible on the same place.

Similarly to traditional telephone sets the information transmitting terminal device 10 has a keyboard, microphone and sound emitter – not shown here – and apart from these it also has a storage partial unit 11, a sender partial unit 18 and a receiver partial unit 19. The storage partial unit 11 also has an ID-register 12 for recording the device identification signal 12a and a D-register 14 containing the information transmitting terminal device's 10 own decoding key 17. The C-register 13 suitable for the temporary or permanent storage of the master coding key 41a of the central traffic co-ordinating unit 40 also belongs here, as well as the temporary storage register 15, which is responsible for storing the coding key 26 of the other terminal device performing actual data traffic – in our case this is the information transmitting terminal device 20 – during the connection. Practically the

temporary storage register 15 of the information transmitting terminal device 10 should be connected to the sender partial unit 18.

Practically the structural construction of the information transmitting terminal device 20 is the same as that of the information transmitting terminal device 10. Similarly to traditional telephone sets it also has a keyboard, microphone and sound emitter – not shown here either – and a storage partial unit 21, a sender partial unit 28 and a receiver partial unit 29. The ID-register 22, the D-register 24 and the temporary storage register 25 belong to the storage partial unit 21. The ID-register records the unique device identifying signal 22a of the information transmitting terminal device 20, while the D-register 24 carries the information transmitting terminal device's 20 own decoding key 27. The coding key 16 of the currently connected information transmitting terminal device 10 – in our case – can be found in the temporary storage register 25. And in this case too the C-register 23 is for the temporary or permanent storage of the master coding key 41a. From the aspect of the information transmitting terminal device 20 it is favourable, if the temporary storage register 25 is in connection with the sender register 28.

In the course of a possible realisation of the operation of the set of equipment the information transmitting terminal device 10 acts as the call initiating unit, and the information transmitting terminal device 20 acts as the called unit, but the set of equipment is also suitable for establishing several signal forwarding connections simultaneously, that is for establishing so-called conference connection.

Dialling the unique identifying number, e.g.: telephone number, of the information transmitting terminal device 20 or the device identifying signal 22a of the information transmitting terminal device 20 on the information transmitting terminal device 10, it sends its login through the information forwarding network to the central traffic co-ordinating unit 40 in a way that the information transmitting terminal device 10 codes the login message with the help of the master coding key 41a situated in the C-register 13 of the information transmitting terminal device, and it furthers the coded signal through the sender partial unit 18 to the central traffic co-ordinating unit 40.

With the help of the master decoding key 42a recorded in its MD-register 42 the central traffic co-ordinating unit 40 disassembles the message coded with the master coding key 41a. On the one part on the basis of the content of the message it identifies the information transmitting terminal device 10 on the basis of its own device identifying signal 12a, and on the other part it checks whether an information transmitting terminal device 20 really belongs to the received device identifying signal 22a, and if yes, according to the device identifying signal 22a it finds the coding key 26 of the information transmitting terminal device 20 in the base cell 43b of the memory unit 43. The central traffic co-ordinating unit 40 encrypts the coding key 26 of the information transmitting terminal device 20 with the help of the coding key 16 of the information transmitting terminal device 10 and sends it to the receiver partial unit 19 of the information transmitting terminal device 10. The receiver partial unit 19 of the information transmitting terminal device 10 disassembles the received information with the help of its decoding key 17 and by this it gains temporary access to the coding key 26 of the information transmitting terminal device, which it stores in the temporary storage register 15 of the information transmitting terminal device.

The call initiating information transmitting terminal device 10 tries to get in contact with the information transmitting terminal device 20 through the information forwarding network 30. If the information transmitting terminal device 10 cannot get in contact with the information transmitting terminal device 20 belonging to the device identifying signal 22a, then the connection cannot be established.

In the case that the information transmitting terminal device 10 has managed to get in contact with the information transmitting terminal device 20, then it sends its own device identifying signal 12a encrypted with the coding key 26 of the information transmitting terminal device 10 to the information transmitting terminal device 20. The information transmitting terminal device 20 disassembles it with its own decoding key 27 and then coding it with the help of the master coding key belonging to the central traffic co-ordinating unit 40 it sends it through the information forwarding network 30 to the central traffic co-ordinating unit 40, and requests the coding key 16 of the information transmitting terminal device 10 from it.

In accordance with the device identifying signal 12a received from the information transmitting terminal device 20 the central traffic co-ordinating unit 40 selects the coding key 16 of the information transmitting terminal device from the base cell 43a of the memory unit 43. Then the central traffic co-ordinating unit 40 encrypts the coding key 16 of the information transmitting terminal device 10 with the help of the coding key 26 of the information transmitting terminal device 20, and sends it to the information transmitting terminal device 20. The information transmitting terminal device 20 receives the encrypted message sent by the central traffic co-ordinating unit 40 in its receiver partial unit 29, disassembles it with its own decoding key 27 as a result of which it gets to know the coding key 16 of the call initiating information transmitting terminal device 10, which it stores temporarily in the temporary storage register 25 of the information transmitting terminal device 20 in a way impossible to read.

After the coding key 16 has been sent to the information transmitting terminal device 20 and the coding key 26 has been sent to the information transmitting terminal device 10 the information transmitting terminal device 10 can encrypt its information to be sent to the information transmitting terminal device 20 with the help of the coding key 26, so that now the information can be sent through the sender partial unit 18 straight to the information transmitting terminal device 20, which in its receiver partial unit 29 receives the data sent from the sender partial unit 18 of the information transmitting terminal device 10 through the information forwarding network 30 – and coded with the coding key 26 of the information transmitting terminal device 20 – it can disassemble it and so it becomes easily interpretable for the person or equipment using the information transmitting terminal device 20.

The information transmitting terminal device 20 can answer the information received from the information transmitting terminal device 10 so that it encrypts the data it intends to send with the help of the coding key 16 situated in the temporary storage register 25, sends it to the sender partial unit 28, from there to the information forwarding network 30, and then it is directly furthered to the receiver partial unit 19 of the information transmitting terminal device 10. It tries to disassemble the data arriving at the receiver partial unit 19 with the decoding key 17 of the information transmitting terminal device 10, and it

succeeds, then the data can be easily interpreted by the person or equipment using the information transmitting terminal device 10.

This direct signal traffic between the information transmitting terminal device 10 and the information transmitting terminal device 20 through the information forwarding network is realised in a way that the central traffic co-ordinating unit 40 does not take part in it. The information transmitting terminal device 10 and the information transmitting terminal device 20 temporarily get to know each other's coding key 16 and coding key 26, and they are able to realise direct information exchange. After the termination of the traffic between information transmitting terminal device 10 and the information transmitting terminal device 20 the coding key 26 situated in the temporary storage register 15 of the information transmitting terminal device 10 is deleted, and the same happens with the coding key 16 situated in the temporary storage register 25 of the information transmitting terminal device 20.

After finishing the call of the information transmitting terminal device 10, in the information transmitting terminal device 20 only its own decoding key 27 situated in the D-register 24 and the master coding key 41a situated in the C-register 23 remain. At the same time the information transmitting terminal device 10 only keeps its own decoding key 17 situated in the D-register 14 and the master coding key 41a situated in the C-register 13.

On the basis of describing the process it can be seen that in the course of establishing data forwarding the information transmitting terminal device 10, the information transmitting terminal device 20 and the central traffic co-ordinating unit 40 do not get in a position even for a moment when they have a coding-decoding key pair belonging together at the same time. So it is not possible for anyone of the users of the set of equipment to have access to the coding key 16 and the decoding key 17, or the coding key 26 and the decoding key 27 at the same time.

It is obvious that the central traffic co-ordinating unit 40 is able to store and administrate network addresses needed for network access, determined by the characteristics of the

information forwarding network 40, and forward the addresses needed for establishing connection towards the information transmitting terminal devices 10 and 20.

In the interest of increasing security even more, it can also be solved that the central traffic co-ordinating unit 40 does not contain the master coding key 41a and the master decoding key 42a at the same time. Knowing only one member of the coding-decoding key pairs makes it impossible to decrypt encrypted messages.

## List of references

10 information transmitting terminal device

11 storage partial unit
12 ID-register
12a device identifying signal
13 C-register
14 D-register
15 temporary storage register
16 coding key
17 decoding key
18 sender partial unit
19 receiver partial unit

20 information transmitting terminal device

21 storage partial unit
22 ID-register
22a device identifying signal
23 C-register
24 D-register
25 temporary storage register
26 coding key
27 decoding key
28 sender partial unit
29 receiver partial unit

30 information forwarding network

40 central traffic co-ordinating unit

41 MC-register
41a master coding key
42 MD-register
42a master decoding key
43 memory unit
43a base cell
43b base cell